

AMENDMENTS TO THE CLAIMS

1 1. (Currently amended) In a system comprising at least one application and a
2 framework, a method performed by the framework comprising:
3 receiving a request from the application for a customized implementation of a
4 service;
5 determining a set of zero or more restrictions to be imposed upon said customized
6 implementation;
7 dynamically constructing said customized implementation, said customized
8 implementation incorporating said restrictions, and comprising enforcement logic for
9 enforcing said restrictions; and
10 providing said customized implementation to the application;
11 wherein said customized implementation is invocable by the application without
12 further interaction with the framework.

1 2. (Cancelled)

1 3. (Original) The method of claim 1, wherein the system further comprises a
2 general implementation for said service, wherein said general implementation is
3 unrestricted, and wherein said customized implementation further incorporates said
4 general implementation.

1 4. (Original) The method of claim 3, wherein said enforcement logic
2 enforces said restrictions on said general implementation.

1 5. (Original) The method of claim 1, wherein said enforcement logic is
2 invoked upon initialization of said customized implementation.

1 6. (Original) The method of claim 5, wherein said enforcement logic, when
2 invoked:
3 receives a set of desired parameters from the application;
4 determines whether the desired parameters exceed said restrictions; and
5 in response to a determination that the desired parameters exceed said restrictions,
6 preventing said customized implementation from operating.

1 7. (Original) The method of claim 5, wherein said service is an
2 encryption/decryption service, and wherein said enforcement logic, when invoked:
3 determines whether a particular exemption mechanism has been invoked; and
4 in response to a determination that the particular exemption mechanism has not
5 been invoked, preventing said customized implementation from operating.

1 8. (Original) The method of claim 1, wherein determining the set of zero or
2 more restrictions comprises:
3 accessing information specifying one or more limitations; and
4 processing said limitations to derive said restrictions.

1 9. (Original) The method of claim 8, wherein said service is an
2 encryption/decryption service, and wherein said information comprises a set of one or
3 more default encryption limitations.

1 10. (Original) The method of claim 9, wherein said default encryption
2 limitations are derived by merging multiple jurisdiction policies and extracting therefrom
3 the most restrictive encryption limitations.

1 11. (Original) The method of claim 1, wherein determining the set of zero or
2 more restrictions comprises:

3 accessing information specifying one or more limitations;
4 determining permissions, if any, granted to the application; and
5 reconciling said limitations and said permissions to derive said restrictions.

1 12. (Original) The method of claim 11, wherein said limitations and said
2 permissions are reconciled to derive restrictions which are least restrictive.

1 13. (Original) The method of claim 11, wherein said service is an
2 encryption/decryption service, and wherein said information comprises a set of one or
3 more default encryption limitations, and a set of zero or more exempt encryption
4 limitations which apply when one or more exemption mechanisms are implemented.

1 14. (Original) The method of claim 13, wherein said default encryption
2 limitations and said exempt encryption limitations are derived by merging multiple
3 jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

1 15. (Original) The method of claim 13, wherein reconciling said limitations
2 and said permissions comprises:

3 determining whether the application has been granted any permissions; and
4 in response to a determination that the application has not been granted any
5 permissions, deriving said restrictions from said set of default encryption limitations.

1 16. (Original) The method of claim 13, wherein reconciling said limitations
2 and said permissions comprises:

3 determining whether the application has been granted any permissions which
4 require implementation of a particular exemption mechanism;

5 in response to a determination that the application has been granted a permission
6 which requires implementation of a particular exemption mechanism, determining
7 whether said exempt encryption limitations allow said particular exemption mechanism
8 to be implemented; and

9 in response to a determination that said exempt encryption limitations allow said
10 particular exemption mechanism to be implemented, deriving said restrictions from said
11 set of exempt encryption limitations.

1 17. (Original) The method of claim 1, wherein the system further comprises a
2 general implementation for said service, and wherein dynamically constructing said
3 customized implementation comprises:

4 instantiating the general implementation to give rise to a general implementation
5 instance;

6 instantiating a wrapper object; and

7 encapsulating said general implementation instance and said restrictions within
8 said wrapper object to derive said customized implementation.

1 18. (Original) The method of claim 17, wherein said wrapper object comprises
2 one or more invocable methods, wherein said general implementation instance comprises
3 one or more invocable methods, and wherein encapsulating comprises:

4 mapping one or more of the invocable methods of said wrapper object to one or
5 more of the invocable methods of said general implementation instance.

1 19. (Original) The method of claim 18, wherein said wrapper object comprises
2 initialization logic for enforcing said restrictions on said general implementation instance.

1 20. (Original) The method of claim 19, wherein said initialization logic is
2 invoked prior to allowing any of the invocable methods of said general implementation
3 instance to be invoked.

1 21. (Original) The method of claim 17, further comprising:
2 instantiating an exemption mechanism to give rise to an exemption mechanism
3 instance; and
4 encapsulating said exemption mechanism instance within said wrapper object.

1 22. (Currently amended) In a system comprising at least one application, a
2 framework comprising:

3 a mechanism for receiving a request from the application for a customized
4 implementation of a service;

5 a mechanism for determining a set of zero or more restrictions to be imposed
6 upon said customized implementation;

7 a mechanism for dynamically constructing said customized implementation, said
8 customized implementation incorporating said restrictions, and comprising enforcement
9 logic for enforcing said restrictions; and

10 a mechanism for providing said customized implementation to the application;
11 wherein said customized implementation is invocable by the application without
12 further interaction with the framework.

1 23. (Cancelled)

1 24. (Original) The framework of claim 22, wherein the system further
2 comprises a general implementation for said service, wherein said general
3 implementation is unrestricted, and wherein the mechanism for dynamically constructing
4 said customized implementation further incorporates said general implementation within
5 said customized implementation.

1 25. (Original) The framework of claim 24, wherein said enforcement logic
2 enforces said restrictions on said general implementation.

1 26. (Original) The framework of claim 22, wherein said enforcement logic is
2 invoked upon initialization of said customized implementation.

1 27. (Original) The framework of claim 26, wherein said enforcement logic,
2 when invoked:
3 receives a set of desired parameters from the application;
4 determines whether the desired parameters exceed said restrictions; and
5 in response to a determination that the desired parameters exceed said restrictions,
6 preventing said customized implementation from operating.

1 28. (Original) The framework of claim 26, wherein said service is an
2 encryption/decryption service, and wherein said enforcement logic, when invoked:
3 determines whether a particular exemption mechanism has been invoked; and
4 in response to a determination that the particular exemption mechanism has not
5 been invoked, preventing said customized implementation from operating.

1 29. (Original) The framework of claim 22, wherein the mechanism for
2 determining the set of zero or more restrictions comprises:
3 a mechanism for accessing information specifying one or more limitations; and
4 a mechanism for processing said limitations to derive said restrictions.

1 30. (Original) The framework of claim 29, wherein said service is an
2 encryption/decryption service, and wherein said information comprises a set of one or
3 more default encryption limitations.

1 31. (Original) The framework of claim 30, wherein said default encryption
2 limitations are derived by merging multiple jurisdiction policies and extracting therefrom
3 the most restrictive encryption limitations.

1 32. (Original) The framework of claim 22, wherein the mechanism for
2 determining the set of zero or more restrictions comprises:
3 a mechanism for accessing information specifying one or more limitations;
4 a mechanism for determining permissions, if any, granted to the application; and
5 a mechanism for reconciling said limitations and said permissions to derive said
6 restrictions.

1 33. (Original) The framework of claim 32, wherein said limitations and said
2 permissions are reconciled to derive restrictions which are least restrictive.

1 34. (Original) The framework of claim 32, wherein said service is an
2 encryption/decryption service, and wherein said information comprises a set of one or
3 more default encryption limitations, and a set of zero or more exempt encryption
4 limitations which apply when one or more exemption mechanisms are implemented.

1 35. (Original) The framework of claim 34, wherein said default encryption
2 limitations and said exempt encryption limitations are derived by merging multiple
3 jurisdiction policies and extracting therefrom the most restrictive encryption limitations.

1 36. (Original) The framework of claim 34, wherein the mechanism for
2 reconciling said limitations and said permissions comprises:

3 a mechanism for determining whether the application has been granted any
4 permissions; and

5 a mechanism for deriving, in response to a determination that the application has
6 not been granted any permissions, said restrictions from said set of default encryption
7 limitations.

1 37. (Original) The framework of claim 34, wherein the mechanism for
2 reconciling said limitations and said permissions comprises:

3 a mechanism for determining whether the application has been granted any
4 permissions which require implementation of a particular exemption mechanism;

5 a mechanism for determining, in response to a determination that the application
6 has been granted a permission which requires implementation of a particular exemption
7 mechanism, whether said exempt encryption limitations allow said particular exemption
8 mechanism to be implemented; and

9 a mechanism for deriving, in response to a determination that said exempt
10 encryption limitations allow said particular exemption mechanism to be implemented,
11 said restrictions from said set of exempt encryption limitations.

1 38. (Original) The framework of claim 22, wherein the system further
2 comprises a general implementation for said service, and wherein the mechanism for
3 dynamically constructing said customized implementation comprises:
4 a mechanism for instantiating the general implementation to give rise to a general
5 implementation instance;
6 a mechanism for instantiating a wrapper object; and
7 a mechanism for encapsulating said general implementation instance and said
8 restrictions within said wrapper object to derive said customized implementation.

1 39. (Original) The framework of claim 38, wherein said wrapper object
2 comprises one or more invocable methods, wherein said general implementation instance
3 comprises one or more invocable methods, and wherein the mechanism for encapsulating
4 comprises:
5 a mechanism for mapping one or more of the invocable methods of said wrapper
6 object to one or more of the invocable methods of said general implementation instance.

1 40. (Original) The framework of claim 39, wherein said wrapper object
2 comprises initialization logic for enforcing said restrictions on said general
3 implementation instance.

1 41. (Original) The framework of claim 40, wherein said initialization logic is
2 invoked prior to allowing any of the invocable methods of said general implementation
3 instance to be invoked.

1 42. (Original) The framework of claim 38, further comprising:
2 a mechanism for instantiating an exemption mechanism to give rise to an
3 exemption mechanism instance; and
4 a mechanism for encapsulating said exemption mechanism instance within said
5 wrapper object.

1 43. (Currently amended) In a system comprising at least one application, a
2 computer readable medium having stored thereon instructions which, when executed by
3 one or more processors, cause the one or more processors to implement a framework
4 which dynamically constructs a customized implementation of a service, said computer
5 readable medium comprising:
6 instructions for causing one or more processors to receive a request from the
7 application for a customized implementation of a service;
8 instructions for causing one or more processors to determine a set of zero or more
9 restrictions to be imposed upon said customized implementation;
10 instructions for causing one or more processors to dynamically construct said
11 customized implementation, said customized implementation incorporating said
12 restrictions, and comprising enforcement logic for enforcing said restrictions; and
13 instructions for causing one or more processors to provide said customized
14 implementation to the application;
15 wherein said customized implementation is invocable by the application without
16 further interaction with the framework.

1 44. (Canceled)

1 45. (Original) The computer readable medium of claim 43, wherein the
2 system further comprises a general implementation for said service, wherein said general
3 implementation is unrestricted, and wherein said customized implementation further
4 incorporates said general implementation.

1 46. (Original) The computer readable medium of claim 45, wherein said
2 enforcement logic enforces said restrictions on said general implementation.

1 47. (Original) The computer readable medium of claim 43, wherein said
2 enforcement logic is invoked upon initialization of said customized implementation.

1 48. (Original) The computer readable medium of claim 47, wherein said
2 enforcement logic, when invoked:
3 receives a set of desired parameters from the application;
4 determines whether the desired parameters exceed said restrictions; and
5 in response to a determination that the desired parameters exceed said restrictions,
6 preventing said customized implementation from operating.

1 49. (Original) The computer readable medium of claim 47, wherein said
2 service is an encryption/decryption service, and wherein said enforcement logic, when
3 invoked:
4 determines whether a particular exemption mechanism has been invoked; and
5 in response to a determination that the particular exemption mechanism has not
6 been invoked, preventing said customized implementation from operating.

1 50. (Original) The computer readable medium of claim 43, wherein the
2 instructions for causing one or more processors to determine the set of zero or more
3 restrictions comprises:

4 instructions for causing one or more processors to access information specifying
5 one or more limitations; and

6 instructions for causing one or more processors to process said limitations to
7 derive said restrictions.

1 51. (Original) The computer readable medium of claim 50, wherein said
2 service is an encryption/decryption service, and wherein said information comprises a set
3 of one or more default encryption limitations.

1 52. (Original) The computer readable medium of claim 51, wherein said
2 default encryption limitations are derived by merging multiple jurisdiction policies and
3 extracting therefrom the most restrictive encryption limitations.

1 53. (Original) The computer readable medium of claim 43, wherein the
2 instructions for causing one or more processors to determine the set of zero or more
3 restrictions comprises:

4 instructions for causing one or more processors to access information specifying
5 one or more limitations;

6 instructions for causing one or more processors to determine permissions, if any,
7 granted to the application; and

8 instructions for causing one or more processors to reconcile said limitations and
9 said permissions to derive said restrictions.

1 54. (Original) The computer readable medium of claim 53, wherein said
2 limitations and said permissions are reconciled to derive restrictions which are least
3 restrictive.

1 55. (Original) The computer readable medium of claim 53, wherein said
2 service is an encryption/decryption service, and wherein said information comprises a set
3 of one or more default encryption limitations, and a set of zero or more exempt
4 encryption limitations which apply when one or more exemption mechanisms are
5 implemented.

1 56. (Original) The computer readable medium of claim 55, wherein said
2 default encryption limitations and said exempt encryption limitations are derived by
3 merging multiple jurisdiction policies and extracting therefrom the most restrictive
4 encryption limitations.

1 57. (Original) The computer readable medium of claim 55, wherein the
2 instructions for causing one or more processors to reconcile said limitations and said
3 permissions comprises:

4 instructions for causing one or more processors to determine whether the
5 application has been granted any permissions; and
6 instructions for causing one or more processors to derive, in response to a
7 determination that the application has not been granted any permissions, said restrictions
8 from said set of default encryption limitations.

1 58. (Original) The computer readable medium of claim 55, wherein the
2 instructions for causing one or more processors to reconcile said limitations and said
3 permissions comprises:

4 instructions for causing one or more processors to determine whether the
5 application has been granted any permissions which require implementation of a
6 particular exemption mechanism;

7 instructions for causing one or more processors to determine, in response to a
8 determination that the application has been granted a permission which requires
9 implementation of a particular exemption mechanism, whether said exempt encryption
10 limitations allow said particular exemption mechanism to be implemented; and

11 instructions for causing one or more processors to derive, in response to a
12 determination that said exempt encryption limitations allow said particular exemption
13 mechanism to be implemented, said restrictions from said set of exempt encryption
14 limitations.

1 59. (Original) The computer readable medium of claim 43, wherein the
2 system further comprises a general implementation for said service, and wherein the
3 instructions for causing one or more processors to dynamically construct said customized
4 implementation comprises:

5 instructions for causing one or more processors to instantiate the general
6 implementation to give rise to a general implementation instance;

7 instructions for causing one or more processors to instantiate a wrapper object;
8 and

9 instructions for causing one or more processors to encapsulate said general
10 implementation instance and said restrictions within said wrapper object to derive said
11 customized implementation.

1 60. (Original) The computer readable medium of claim 59, wherein said
2 wrapper object comprises one or more invocable methods, wherein said general
3 implementation instance comprises one or more invocable methods, and wherein the
4 instructions for causing one or more processors to encapsulate comprises:
5 instructions for causing one or more processors to map one or more of the
6 invocable methods of said wrapper object to one or more of the invocable methods of
7 said general implementation instance.

1 61. (Original) The computer readable medium of claim 60, wherein said
2 wrapper object comprises initialization logic for enforcing said restrictions on said
3 general implementation instance.

1 62. (Original) The computer readable medium of claim 61, wherein said
2 initialization logic is invoked prior to allowing any of the invocable methods of said
3 general implementation instance to be invoked.

1 63. (Original) The computer readable medium of claim 59, further
2 comprising:
3 instructions for causing one or more processors to instantiate an exemption
4 mechanism to give rise to an exemption mechanism instance; and
5 instructions for causing one or more processors to encapsulate said exemption
6 mechanism instance within said wrapper object.

1 64. (New) The method of claim 1, wherein said framework comprises Java
2 Cryptography Extension to Java Platform.

1 65. (New) The framework of claim 22, wherein said framework comprises
2 Java Cryptography Extension to Java Platform.

1 66. (New) The computer readable medium of claim 43, wherein said
2 framework comprises Java Cryptography Extension to Java Platform.
